SIPRNet Contractor Accreditation Process (SCAP)

INDUSTRY

Contractor Accreditation Process

1. *Government Sponsor* submits validation letter to Joint Staff (J6)
2. After OSD approval, *J6* emails validation to DISA, DSS & Sponsor
3. *DISA* assigns DISA control number (CXXXXXX) and emails J6 letter to DSS Program Manager (PM)
4. *DSS PM* emails sponsor letter to the Sponsor & field letter to IS Rep
5. *Contractor* prepares SSP and SCQ
6. *DSS IS Rep and ISSP* works with contractor for SSP preparation
7. Contractors can now submit Master Security Plans that identify self-certification of like systems. Note: *DISA issues IP Addresses to the Sponsor. Contractors are then provided a block of IP addresses (based on current sponsor requirements) from their sponsor and they must stay within that range. Additional IP Addresses must be requested by the Sponsor.*
8. *DSS IS Rep* provides completed Certification Package to DAA for final accreditation and signature (No Interims) Includes SSP w/Topology (connectivity diagram) and SCQ
9. *DSS* emails/mails signed DAA Accreditation letter and DAA signed SCQ to the contractor
10. *Contractor* emails/mails completed Connection Package to DISA. Includes SSP, DSS DAA accreditation letter, Statement of Residual Risk with ISSM signature, Letter of Consent with ISSM signature, System Connectivity Diagram and SIPRNet Connection Questionnaire with DSS DAA signature.
11. *DISA* sends email acknowledgement of receipt to the contractor
12. *DISA* reviews Connection Package and if correct issues IATC. If not correct DISA will correspond with the contractor to resolve issues
13. *DISA* emails IATC to contractor and DSS PM
14. *DISA* runs vulnerability test (time period undetermined)
15. When system test passes, *DISA* issues ATC and emails ATC to the contractor

Open Email and Domain Name (DNS) Registration

DSS will no longer be responsible for providing this service to contractors. Starting in FY 2007 sponsors will be required to provide these services to the contractor.

Disclosure Form

Contractors are NOT allowed unfiltered access to the SIPRNet. The DoD Sponsor determines access requirements. Joint Staff letter must identify access requirements (i.e., websites and ports and protocols.)

1. *Sponsor* sends disclosure form received from DSS PM to sites that contractors need access to
2. *Site* agrees, signs the form and submits it back to the Sponsor
3. *Sponsor* sends form to SMC smc-ctr@disa.mil
4. *DISA SMC* builds/updates contractor filter

Re-Accreditation

When authorization expires the system is no longer legal and must be terminated (looped-away). These are steps to extend the life of your system. Be advised to update packages with current information (dates, POC, system changes)

1. If *Joint Staff validation* expires then **Sponsor action required.** Follow Contractor Accreditation Process steps 1,2
2. If *contract* expires then **Sponsor action required.** Submit extension letter to contractor. Contractor must submit extension letter to DSS. Follow Contractor

Accreditation Process steps 1,2 & 5-15

3. If *accreditation* expires then the **Contractor** must obtain a new Accreditation letter from DAA and submit it to DISA. Follow steps 5-15

Points of Contact

Defense Security Service:

Email disn@dss.mil
Address: Defense Security Service
1340 Braddock Place
Alexandria, VA 22314

DISA SIPRNET Connection Approval Office:

Email: scao@ncr.disa.mil
Address: Defense Information Systems Agency
ATTN: GS213/SCAO
P.O. Box 4502
Arlington, VA 22204-4502

Joint Staff:

Email: joyce.bernard@js.pentagon.mil

Disclosure Authorization Office:

Email: smc-cntr@disa.mil